From non-local games to quantum groups

Matthew Daws

Lancaster University

Lancaster, April 2024

Refereed games

Alice and Bob play a game against a referee.

- All the rules are known in advance, and Alice and Bob can agree on a strategy, but in each round they cannot communicate.

Given finite sets X, Y (the questions) and A, B the answers.

- In each round, the referee picks $(x, y) \in X \times Y$ at random (distribution $\pi(x, y)$) and sends x to Alice, and y to Bob.
- Alice replies with $a \in A$, and Bob replies with $b \in B$.

The *rule function* is

$$V : A \times B \times X \times Y; (a, b, x, y) \mapsto V(a, b|x, y) \in \{0, 1\}.$$

$V(a, b|x, y) = 1$ means Alice and Bob win; otherwise they lose.

Example: Graph colouring

Let $G = (V, E)$ be a finite simple graph, consisting of:

- vertices V;
- simple undirected edges E; write $x \sim y$.
- Recall that a *colouring* of a graph is an assignment of colours to each vertex such that adjacent vertices are coloured differently.

Set question set $X = Y = V$ and answer set $A = B = \{1, 2, \cdots, c\}$.

> *Alice and Bob win if they can convince the referee they have a colouring using c colours.*

$$V(a, b|x, y) = \begin{cases} 1 & : x = y, a = b, \\ 0 & : x = y, a \neq b, \\ 0 & : x \sim y, a = b, \\ 1 & : \text{otherwise.} \end{cases}$$

How to win?

How can Alice and Bob always win?

- Need to know $\pi(x, y)$.
- Simplify things: assume $\pi(x, y)$ has full support.

Definition

A “deterministic strategy” is for Alice and Bob to agree on functions

$$f\colon X \to A; \quad g\colon Y \to B,$$

and to always reply $(f(x), g(y))$.

In the graph colouring game, they fix a colouring $f = g$ in advance, and always use this.

- Always satisfies “same question, same answer” rule.
- Actually must be a colouring to satisfy other rule.

Random strategies

Definition

A "random strategy" is to pick a probability space $(\Omega, \mathbb{P})$ and for each $\omega \in \Omega$ have deterministic strategies f_ω, g_ω.

Alice and Bob agree in advance some random numbers, and so can sample from the space without communicating. They can now give a random answer

$$p(a, b|x, y) = \mathbb{P}\big(\omega : f_\omega(x) = a, g_\omega(y) = b\big).$$

Instead, for each $x \in X$ define

$$F_x \colon \Omega \to A; \quad F_x(\omega) = f_\omega(x),$$

similarly G_y. Then F_x, G_y are random variables, with

$$p(a, b|x, y) = \mathbb{P}\big(\omega : F_x(\omega) = a, G_y(\omega) = b\big).$$

Random strategies cont.

$$p(a, b|x, y) = \mathbb{P}\big(\omega : F_x(\omega) = a, G_y(\omega) = b\big).$$

So having a random mixture of deterministic strategies is the same as, for each input, having a random variable to sample your output from.

$$\mathbb{E}\, V = \sum_{x,y} \pi(x, y) \sum_{a,b} p(a, b|x, y)\, V(a, b|x, y).$$

As we assume $\pi(x, y) > 0$ for all x, y, if $\mathbb{E}\, V = 1$ then

$$\sum_{a,b} p(a, b|x, y)\, V(a, b|x, y) = 1,$$

for all x, y, and so

Definition

A *perfect strategy* is one satisfying

$$V(a, b|x, y) = 0 \quad \implies \quad p(a, b|x, y) = 0.$$

Random doesn't help

Everything is finite, so the σ-algebra generated by F_x, G_y is finite, so really we have a finite mixture of deterministic strategies:

- pick $f_i \colon X \to A, g_i \colon Y \to B$ with probability p_i.

$$\mathbb{E}\,V = \sum_{i=1}^{N} p_i \sum_{x,y} \pi(x,y)\, V(f_i(x), g_i(y)|x,y).$$

- Picking the i which maximises the inner sum gives a deterministic strategy which is at least as good as this random strategy.

In Applications, however, Alice and Bob might want to deliberately give random answers, to avoid the referee learning too much.

Quantum mechanics

A mathematical model of quantum mechanics is that the state of a quantum system is described by a unit vector ψ in a $\mathbb{C}$-inner product space (Hilbert space) $\mathcal{H}$.

Definition

A qubit is a unit vector $\psi \in \mathbb{C}^2$.

Basis

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Or maybe use the "spin" $|\uparrow\rangle, |\downarrow\rangle$. We can of course have mixtures

$$\psi = \begin{pmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{pmatrix} = \tfrac{1}{\sqrt{2}}|\uparrow\rangle - \tfrac{1}{\sqrt{2}}|\downarrow\rangle.$$

Measurement

We cannot observe the state of a system directly, only "measure" it. This is defined by a self-adjoint operator (a matrix) A acting on $\mathcal{H}$. Perhaps we measure spin up as 1 and spin down as -1, so

$$A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

So A has:

- $|\uparrow\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ as an eigenvector for eigenvalue $+1$, and
- $|\downarrow\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ as an eigenvector for eigenvalue -1.

When we measure a state ψ, we obtain a probabilistic outcome:

- Express ψ in the unit-vector eigenbasis which diagonalises A.
- ψ is a unit vector, so the coefficients in this basis have squares which sum to 1: these are the probabilities.

Example

$$A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad \psi = \begin{pmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{pmatrix} = \tfrac{1}{\sqrt{2}}|\uparrow\rangle - \tfrac{1}{\sqrt{2}}|\downarrow\rangle.$$

- With probability $1/2$ we obtain $+1$, and ψ collapses into $|\uparrow\rangle$.
- With probability $1/2$ we obtain -1, and ψ collapses into $|\downarrow\rangle$ (or $-|\downarrow\rangle$).

If instead

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

then eigenvalue 1 has eigenbasis spanning the whole space, and we instead take the *orthogonal projection* of ψ onto this *eigenspace*.

- In this case, the projection is onto the whole space, so we always get the measurement 1, and ψ does not change.

Entanglement

The product of two systems is modelled by taking the tensor product of the state spaces. So two qubits has a $2 \times 2 = 4$ dimensional state space with basis

$$|\uparrow\rangle \otimes |\uparrow\rangle = |\uparrow\uparrow\rangle, \quad |\uparrow\rangle \otimes |\downarrow\rangle = |\uparrow\downarrow\rangle, \text{ and } |\downarrow\uparrow\rangle, \ |\downarrow\downarrow\rangle.$$

If we measure one system using A, this is the same as measuring the whole system using $A \otimes I$. E.g. consider the "Bell state"

$$\psi = \frac{1}{\sqrt{2}}\big(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle\big), \text{ with } A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Measuring the first qubit:

- with probability $1/2$ we get $+1$, and project onto eigenbasis $\{|\uparrow\uparrow\rangle, |\uparrow\downarrow\rangle\}$, so ψ collapses to $|\uparrow\downarrow\rangle$;
- with probability $1/2$ we get -1, and project onto eigenbasis $\{|\downarrow\uparrow\rangle, |\downarrow\downarrow\rangle\}$, so ψ collapses to $|\downarrow\uparrow\rangle$ (or $-|\downarrow\uparrow\rangle$).

Spooky action at a distance

Alice and Bob share the state ψ in different labs (in 2023, circa 30 metres). If Alice performs this measurement, then with 50-50 chance, she finds:

- ψ collapses to either $|\uparrow\downarrow\rangle$ or $|\downarrow\uparrow\rangle$; and she measures
- $+1$ with her qubit collapsing into $|\uparrow\rangle$ and Bob's qubit collapsing into $|\downarrow\rangle$;
- -1 with her qubit collapsing into $|\downarrow\rangle$ and Bob's qubit collapsing into $|\uparrow\rangle$.

"Non-locality" but no information passes.

Aim: use our games with "quantum correlations" to explore this non-local behaviour.

PVMs

Measurement can be abstracted to:

- Write $\mathcal{H}$ as a sum of orthogonal subspaces;
- express a state in this direct sum decomposition.

The operator projecting onto a subspace is a *projection* which is a self-adjoint p with $p^2 = p$. A direct sum decomposition corresponds to projections $p_1, \cdots, p_n$ with

$$\sum_{k=1}^{n} p_k = 1 \quad \implies \quad p_i p_j = p_j p_i = 0 \ (i \neq j).$$

Definition

Such a family $(p_i)_{i=1}^{n}$ is a *projection valued measure* or PVM.

Given a state ψ, the probability of measuring output k is simply

$$(\psi | p_k \psi) = (\psi | p_k^2 \psi) = (p_k \psi | p_k \psi) = \|p_k \psi\|^2.$$

[Mention POVMs?]

Quantum correlations

Definition

A *quantum correlation* is described by Hilbert spaces $\mathcal{H}_A, \mathcal{H}_B$ for Alice and Bob, a shared state $\psi \in \mathcal{H}_A \otimes \mathcal{H}_B$, and for each input $x \in X$ a PVM $(P_a^x)_{a\in A}$, and similarly $(Q_b^y)_{b\in B}$. The associated correlation is

$$p(a,b|x,y) = \big(\psi \big| (P_a^x \otimes Q_b^y)\psi\big).$$

If ψ is *separable*, $\psi = \psi_A \otimes \psi_B$, then

$$p(a,b|x,y) = (\psi_A|P_a^x\psi_A)(\psi_B|Q_b^y\psi_B)$$

which are just probabilities, so we're back to a random mixture of deterministic strategies, a "local strategy".

Approximate quantum correlations

Typically we have $X = Y, |X| = n$ and $A = B, |A| = k$.

Definition

Let $C_{loc}(n,k)$ and $C_q(n,k)$ be the sets of correlation functions $p(a,b|x,y)$ arising from local strategies, respectively, quantum strategies.

Theorem (Bell 1964, CHSH 1969)

$C_{loc}(n,k) \subsetneq C_q(n,k)$ *even for* $n = k = 2$*.*

As these are spaces of functions from a finite set to $[0,1]$ there is a topology, and we can define $C_{qa}(n,k)$ to be the closure of $C_q(n,k)$ (i.e. correlations we can *approximate* by quantum correlations.)

Theorem (Slofstra, 2019)

$C_q(n,k) \subsetneq C_{qa}(n,k)$ *for sufficiently large* n,k*.*

Commuting quantum correlations

We replace $\mathcal{H}_A \otimes \mathcal{H}_B$ by some abstract Hilbert space $\mathcal{H}$.

- Then "$P^x_a \otimes Q^y_b$" no longer makes sense.
- Instead, pick PVMs $(P^x_a)_{a\in A}$ and $(Q^y_b)_{b\in B}$ both acting on $\mathcal{H}$, and insist they pairwise commute: $P^x_a Q^y_b = Q^y_b P^x_a$ for each a, b.

If $\mathcal{H}$ is still finite-dimensional, this gives us nothing new (non-obvious...)

So, let $\mathcal{H}$ be infinite-dimensional. $C_{qc}(n,k)$ is the resulting "quantum commuting correlations".

Theorem (Ji, Natarajan, Vidick, Yuen, 2022??)

MIP=RE which implies $C_{qa}(n,k) \subsetneq C_{qc}(n,k)$ for large enough n, k. As a corollary, the Connes Embedding problem is false.*

Non-signalling correlations

[Skip?]
Stepping away from quantum theory...

Definition

A correlation $p(a, b|x, y)$ is *non-signalling* when:

1. $(a, b) \mapsto p(a, b|x, y)$ is a probability;
2. $P_A(a|x) = \sum_b p(a, b|x, y)$ is independent of y;
3. $P_B(b|y) = \sum_a p(a, b|x, y)$ is independent of x.

This captures the idea that Alice and Bob cannot communicate. I imagine an "oracle" which Alice and Bob send their inputs x, y to, and the oracle replies with a, b. That $P_A(a|x)$ is well-defined means that Alice cannot learn about y or b even by observing which values a she gets from her inputs x.

Back to graph colouring

We only look at perfect strategies, where Alice and Bob can always win.

$$V(a, b|x, y) = 0 \implies p(a, b|x, y) = 0.$$

Definition

Given a graph G let $\chi(G)$ be the *chromatic number* of G, the smallest number of colours needed for a vertex colouring.
Let $\chi_t(G)$ be the smallest number of colours needed for a perfect strategy for the graph colouring game, using $t \in \{loc, q, qa, qc\}$.

Proposition

$\chi(G) = \chi_{loc}(G)$

Hadamard Graphs

The *Hadamard graph* Ω_N has vertex set all vectors in $\{\pm 1\}^N$ (so $|V| = 2^N$) and $u \sim v$ when $u \cdot v = 0$.

Theorem (DeKlerk–Pasechnik 2005)

$\chi(\Omega_{16}) \geqslant 29$.

Theorem (Avis-Hagasawa-Kikuchi-Sasaki, 2006)

$\chi_q(\Omega_N) \leqslant N$ *for all (even)* N.

Lots of recent work on χ_q.

I *think* that it's not known if the graph colouring game can distinguish q from qa (or qa from qc).

Synchronous Games and algebras

As usual, $X = Y, A = B$.

Definition

A game is *synchronous* when $V(a, b|x, x) = 0$ whenever $a \neq b$. (Same question must lead to same answer.)

Theorem (Paulsen et al. 2016)

In a perfect (q, qa, qc) strategy for a synchronous game, we may suppose that $P_a^x = Q_a^x$ *for all* x *and* a.
If we consider the C^**-algebra generated by all the* P_a^x*, then* $X \mapsto (\psi|X\psi)$ *is a trace.*

C^*-algebras

We have a collection A of operators on a Hilbert space $\mathcal{H}$ (in finite-dimensions, just a collection of square matrices) which is:

- An algebra, so a vector space where multiplication makes sense: $x, y \in A \implies xy \in A$;
- self-adjoint, so $x \in A \implies x^* \in A$;
- there is a norm: $\|x\|^2 = \|x^*x\|$ where x^*x is positive (all eigenvalues are positive) and $\|x^*x\|$ is the largest eigenvalue;
- A is closed for the topology induced by this norm.

A *trace* is a (bounded) map $\tau\colon A \to \mathbb{C}$ with $\tau(xy) = \tau(yx)$.

Game algebras

We can analyse a synchronous game $\mathcal{G}$ by looking at its “game algebra” $A(\mathcal{G})$.

- This algebra is generated by elements $e_{x,a}$, for $x \in X$, $a \in A$, with the relations:
  - each $e_{x,a}$ is a projection: $e_{x,a} = e_{x,a}^* = e_{x,a}^2$;
  - for each x we have $\sum_a e_{x,a} = 1$.
- with further relations that $V(a,b|x,y) = 0 \implies e_{x,a} e_{y,b} = 0$.

Aside: the algebra generated by projections $e_1, \cdots, e_n$ with $\sum_k e_k = 1$ is $C([n]) \cong \mathbb{C}[C_n]$ the group algebra of the cyclic group of order n, via the Fourier transform. So the free algebra we consider is

$$C([n]) \star \cdots \star C([n]) \cong \mathbb{C}(C_n \star \cdots \star C_n)$$

the group algebra of a free product of cyclic groups.

Building deterministic strategies

Let $\theta\colon A(\mathcal{G}) \to \mathbb{C}$ be a unital $*$-homomorphism.

- So $\theta(e_{x,a}) \in \mathbb{C}$ is a projection, so must equal 0 or 1;
- that $\sum_a \theta(e_{x,a}) = 1$ means that for each x there is exactly one a with $\theta(e_{x,a}) = 1$; call this $f(x)$.
- $V(a,b|x,y) = 0 \implies \theta(e_{x,a})\theta(e_{y,b}) = 0$ so $a \neq f(x)$ or $b \neq f(y)$ so $(a,b) \neq (f(x),f(y))$
- contrapositive: $(a,b) = (f(x),f(y)) \implies V(a,b|x,y) = 1$
- that is, $V(f(x),f(y)|x,y) = 1$ for all x,y.
- i.e. f is a perfect deterministic strategy.

Similarly, a quantum strategy arises from a $*$-homomorphism $A(\mathcal{G}) \to \mathbb{M}_n$. A quantum commuting strategy arises from a $*$-homomorphism $A(\mathcal{G}) \to A$ for some C^*-algebra admitting a faithful state. (qa strategies arise from $\mathcal{R}^\omega$.)

Graph homomorphism game

Consider now two graphs $G = (V_G, E_G)$ and $H = (V_H, E_H)$. A *homomorphism* is a function $f \colon V_G \to V_H$ with $x \sim y$ in G implying that $f(x) \sim f(y)$ in H.

We can define a game with input set V_G and output set V_H. Alice and Bob need to convince the referee they really have a graph homomorphism $G \to H$, so

$$V(a, b|x, y) = \begin{cases} 0 & : x = y, a \neq b, \\ 0 & : x \sim y, a \nsim b, \\ 1 & : \text{otherwise.} \end{cases}$$

This game can distinguish qa and q (using an “artificial” graph built from the binary constraint satisfaction game Slofstra used to show $C_{qa} \neq C_q$.)

Graph isomorphism game

We now set both input and output sets to be $V_G \cup V_H$ (disjoint union). The players must convinced the referee they have an isomorphism between the graphs. Classically this would be $f \colon V_G \to V_H$ so that $x, y \in V_G$ have the same "relation" as $f(x), f(y)$ in V_H.

> *"relation" means one of "equal", "adjacent", "not adjacent".*

The game algebra generators $e_{x,a}$ form a square matrix which ends up having the form

$$(e_{x,a}) = \begin{bmatrix} 0 & f \\ f^\top & 0 \end{bmatrix} \quad \text{where} \quad f = (f_{x,y})_{x\in V_G, y\in V_H}.$$

Then f is a "quantum permutation" aka "magic unitary":

- each entry $f_{x,y}$ is a projection,
- rows *and* columns sum to 1.

Finally, $fA_H = A_G f$ where A_G, A_H are the adjacency matrices of G, H.

To quantum groups

Consider O_n^+ the $*$-algebra generated by the entries of a quantum permutation matrix of size n.

- This has extra structure:

$$\Delta\colon f_{x,y} \mapsto \sum_z f_{x,z} \otimes f_{z,y}, \quad S(f_{x,y}) = f_{y,x}, \quad \epsilon(f_{x,y}) = \delta_{x,y}$$

  turn O_n^+ into a Hopf-algebra.
- There is a tracial state which makes O_n^+ into a CQGA: the algebraic version of a compact quantum group.

Compact quantum groups are non-commutative objects which generalise the (commutative) function algebras on compact groups. O_n^+ is the quantum permutation group, objects which have a rich combinatorial structure.

Insisting that f commutes with A_G, the adjacency matrix of a graph, leads to a quotient algebra, the *quantum automorphism group* of G.

Isomorphisms

So the graph isomorphism game is a natural generalisation of the quantum automorphism group of a single graph.
Somewhat a surprise that the same idea turns up!

Theorem (Mančinska–Roberson)

For graphs G, H the following are equivalent:

- *G, H are "quantum isomorphic": there is a perfect qc strategy for playing the graph isomorphism game;*
- *for any planar graph K, the number of graph homomorphisms from K to G, respectively H, agree.*

The proof uses analysis of the representation theory of O_n^+ and related ideas.